511.825

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 03/094424 A1

(51) International Patent Classification[7]: H04L 12/00, 9/00

(21) International Application Number: PCT/IB02/02825

(22) International Filing Date: 3 May 2002 (03.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 ESPOO (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PIETILAINEN, Antti** [FI/FI]; Holmanmaentie 3A, FIN-02240 Espoo (FI). **HIIRONEN, Olli-Pekka** [FI/FI]; Leppakertuntie 3 A 11, FIN-02120 Espoo (FI).

(74) Agents: **SLINGSBY, Philip, Roy** et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

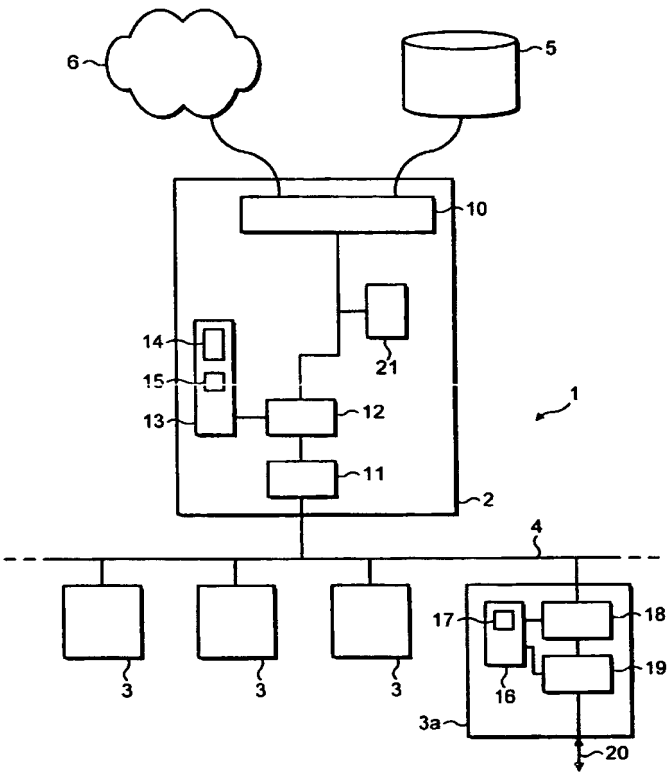
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A METHOD AND SYSTEM IN A COMMUNICATION NETWORK FOR ALLOCARING AND CHANGING LINK-LEVEL ADDRESSES



(57) Abstract: A communication system comprising: a plurality of communication nodes connected by a data link; a communication controller for allocating link-level addresses to the communication nodes whereby the nodes may be identified for communications over the link; the communication controller being arranged to change from time to time the addresses allocated to each communication node and transmit the newly allocated address to the respective node in encrypted form.

WO 03/094424 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD AND SYSTEM IN A COMMUNICATION NETWORK FOR ALLOCARING AND CHANGING LINK-LEVEL ADDRESSES

This invention relates to changing the addresses of entities in a communication network.

When data is being transferred over a communication network it is often important to protect the data from being accessed by an unauthorised person. Often the data is encrypted to prevent it from being read by someone who does not have a key to decrypt it. This kind of hostile hacking of other user's data may also be called sniffing or eavesdropping. But in addition to the data itself there is other ancillary information that may be of use to an unauthorised person who has access to the network. This could include information on the type, timing or amount of traffic being sent to particular entities in the network: it may give clues that could assist a hacker to breach the network's security, or in a commercial network it could reveal sensitive commercial information about the level to which the network is being utilised.

The problems of protecting against access to data and ancillary information are especially acute in shared media networks. In a shared media network a number of entities are connected to each other by a common data link, and data intended for one or more of the entities is broadcast over the link. If it is intended that only one of the entities should receive certain data then a broadcast and select scheme can be used. To implement this scheme each entity has a link-level address in the network and the data is transmitted in conjunction with the link-level address of the entity for which it is intended. When an entity recognises that its link-level address is transmitted in conjunction with an amount of data it decodes that data.

US 6,028,933 describes a method for encrypting data over a shared media multiple access network. This document suggests improving security by full encryption of all downstream bits.

Shared media networks offer a cost-effective way of implementing a network for providing a number of nodes with access to a resource such as the internet. In such a situation the network can comprise a single high-speed transceiver in an access node or hub, which is capable of communicating with many nodes at consumers' premises. A single shared high-speed bus connects the hub to the consumer nodes (also known as satellite nodes). The satellite nodes need a high-speed interface to receive information over the link, but the rest of the electronics at the satellite nodes can be slower and therefore relatively inexpensive. The network can take any suitable topology, for example star, tree, ring, loop or linear. Since all nodes are connected to the same high-speed bus they can listen to traffic that is not intended for them. Even if the data is encrypted, a listening node could detect ancillary information that could be valuable: for instance it could identify how much data is addressed to each other entity and when it is sent. In addition, if the listener wanted to read communications to a particular node he could intercept transmissions that are addressed to that node and store them for decrypting later using a powerful computer.

Wireless shared media networks are especially at risk from this form of monitoring since it is difficult to prevent physical access to the data channel. For example, in IEEE802.11b wireless LAN networks any compatible receiver within range of the hub can listen to transmissions intended for other entities in the network.

One solution to these problems is for consumers or network operators who are concerned about privacy to use a dedicated link between the hub and each node. However, this is expensive.

There is therefore a need to improve the security of networks by making it more difficult for a listener to access ancillary data on network usage.

According to one aspect of the present invention there is provided a communication system comprising: a plurality of communication nodes connected by a data link; a communication controller for allocating link-level addresses to the communication

nodes whereby the nodes may be identified for communications over the link; the communication controller being arranged to change from time to time the addresses allocated to each communication node and transmit the newly allocated address to the respective node in encrypted form.

Most preferably the communication controller is arranged to change the addresses from time to time during a period whilst communication with the nodes is taking place over the data link. Such communication may be discontinuous, and is most preferably packet-based communication. Such communication may suitably be traffic data communication between the communication controller and the or each node.

The data link is preferably a shared data link. The shared data link is shared between the nodes so that any node connected to the data link has access to communications over the link. Suitably each node is arranged to interpret only the communications over the node that are addressed to it. The data link may take any suitable topology. The data link may, for example, be a cable link or a wireless link.

Further aspects of the invention are set out in the dependent claims.

The present invention will now be described by way of example with reference to the accompanying drawings.

In the drawing:

figure 1 is a schematic diagram of a data transmission system, showing components of a hub and a terminal in detail.

In the data transmission system of figure 1 there is a network in which procedures are implemented to inhibit access by a listener to ancillary data on network usage. Receiving devices in the network are allocated link-level addresses for use in the network, and the link-level addresses are changed from time to time so that it is problematic for a listener to determine which entities have which addresses. This

means that it is difficult for the listener to derive ancillary information on usage of the network. Additional procedures, which are described in more detail below, are also used to supplement the security of this procedure.

In figure 1 there is a network shown generally at 1, which comprises a hub 2 and a set of satellite nodes 3. One of the satellite nodes: 3a, is shown in more detail than the others. The satellite nodes are connected to the hub by a shared high-speed data bus 4. The hub 2 is connected to further data resources, for example a local data store 5 and the internet 6.

In practice the satellite nodes could, for example, be personal computers or set-top boxes arranged to receive data from the data bus. The data bus could be an optical fibre link installed to consumers' premises. Instead of a data bus, the shared media may comprise a wireless interface such as radio or optical interface, for instance.

In figure 1 components of the hub 2 and one of the nodes 3a are shown in more detail. The hub comprises an interface 10 by which it is connected to the upstream data resources 5, 6; and an interface 11 by which it is connected to the data bus 4. Interface 10 could be an Ethernet switch or IP router. Interface 11 could be an optical transceiver. Data passing between interfaces 10 and 11 passes through a converter 12, which operates under the control of a link controller 13. The link controller has a store 14 in which it maintains a register of the information needed for communication in the network with each of the nodes 3. That comprises a list of, for each of the nodes 3: the link-level address in the network 1 that is assigned to that node, and the encryption/decryption key(s) assigned to that node. Other information may also be stored to support additional security protocols, for instance the MAC address of the respective node.

The hub 2 may perform address translation so that the nodes 3 are represented to the upstream resources by the address of the hub.

When data from interface 10 is to be sent to one of the satellite nodes it is passed to the converter 12 which operates under the control of the link controller 13 to form a message for transmission over link 4. The link controller provides the converter with the link-level address of the destination node and the encryption key for transmissions to that node. The converter encrypts the data using the encryption key and forms the message so as to be addressed to the node's address. The message is then passed to interface 11.

When data from interface 11 is to be sent to an upstream resource it is passed to the converter 12 which operates under the control of the link controller 13 to form a message for upstream transmission. The converter informs the link controller of the link-level address from which the data was sent. The link controller retrieves from store 14 the appropriate decryption key and provides it to the converter. The converter then decrypts the data using the decryption key and passes the data to interface 11.

At each satellite node 3 there is a transceiver controller 16. The transceiver controller 16 includes a store 17 which stores the link-level address and the encryption/decryption key(s) allocated to the node. The transceiver controller is connected to a data selector 18 and an encryption/decryption unit 19. The data selector 18 is informed by the transceiver controller 16 of the address allocated to the node. The data selector monitors data on link 4 for messages addressed to that node. Any such messages are passed to the encryption/decryption unit 19. It decrypts the messages using the decryption key provided to it by the transceiver controller 16 and then passes the data on for local use (see link 20). When data is received over link 20 for transmission over link 4 the data passes to encryption/decryption unit 19, which encrypts the data using the node's encryption key (as provided by transceiver controller 16) and then passes it to hub 2 via link 4.

Hub 1 also includes a link security controller 15. The link security controller adapts the operation of the network over data bus 4.

The link security controller controls the allocation of link-level addresses to the nodes 3. The link security controller has a pool of addresses available to it and stores a record of which of those have been allocated to nodes 3. When a new node connects to the network it is allocated one of the unallocated addresses from the pool. Additionally, from time to time the link security controller changes the addresses allocated to the nodes. It does this by selecting another unallocated address from the pool, passing it to the node whose address is to be changed and then storing that address as being allocated and the address previously allocated to that node as being unallocated. When an address is allocated to a node it stores it in store 17 and then uses it as described above.

When the link security controller 15 allocates an address to a node it transmits that address to the node in encrypted form, by means of the previously established encryption system using units 11 and 18. Thus nodes listening on link 4 cannot determine the new address allocated to the node. This may be impossible when the node is first allocated an address since at that stage encryption may not have been established for that node. In that situation the security controller allocates the node's initial address in plain transmission and then, once encryption has been established, allocates another address over the encrypted channel.

The link security controller determines when to change the addresses allocated to nodes. It may do so randomly or pseudo randomly, or periodically. It is preferred that it changes the nodes' addresses one by one at random intervals. The time between address changes can conveniently be selected to balance the increased security that derives from the address change with the additional traffic and processing involved in an address change. This will depend on the network conditions.

The link security controller selects new addresses randomly or pseudo randomly from the pool of addresses.

As a result of these features, someone listening on the link 4 cannot easily keep track of which address is allocated to which node. Therefore, he cannot monitor what volume of traffic is passing to which node.

When an address is changed the store 14 is updated. There are two options. If the node whose address is changed is to keep the same encryption key as it had before then the list in store 14 is updated to associate that node's new address with its previous key or key pair. Alternatively, the node's encryption key may be changed at the same time as its address is changed. In that case the record stored in store 14 for the previous address is deleted and a new record is added to associate the new address with the new key or key pair.

To provide additional security, the hub 2 may be arranged to transmit data to the nodes in a random or pseudo random order. The data is sent to the nodes in discrete units, such as frames or packets. When such data is to be transmitted to the nodes the order in which the units are sent is determined at random (or pseudo randomly) by the hub 2. Then the order in which the nodes are addressed is substantially unpredictable to a listener on the link. This provides additional security.

The network has a further security feature. Traffic generator 17 (21) is capable of generating spurious traffic that can be carried over link 4. It does this during times when the link would otherwise be idle. The spurious traffic could have any content, but it is conveniently random or pseudo random. The spurious traffic is formed into addressed messages, as for other traffic over the link, but is addressed to addresses that are unallocated, so that it is not picked up by any of the nodes. The result of this is that a listener on the link cannot tell how much traffic there is on the link, because the link appears to be fully or almost fully utilised all the time.

The systems described above are most conveniently implemented in packet-switched networks, although they could also be used in networks of other types.

One suitable platform for implementing the systems described above is the Ethernet Passive Optical Network (EPON) currently being standardised in the IEEE802.3ah Ethernet First Mile (EFM) task force.

Ethernet PON is a point-to-multipoint network used to send Ethernet frames. It is planned to use the broadcast and select method for downstream traffic and a time division multiple access method for upstream traffic. There will be a PHY ID address which will be used in broadcasting Ethernet frames to destination nodes and whereby the destination nodes can select the frames they should decode. The PHY ID will be included at the beginning of an Ethernet frame. The structure of the Ethernet frame will then be:

PHY ID
MAC ADDRESS
---FIELDS---
---DATA---
---OTHER FIELDS---

All information except the PHY ID is to be encrypted. The PHY ID is an identifier that identifies which node is to receive the frame. The PHY ID thus also indicates which encryption and decryption keys are to be used for the frame.

In a system of this type the process for changing the PHY ID to implement the address changing function of the security controller 15 as described above is:

1. A "New PHY ID" command is sent to the destination node whose address is to be changed. The command is sent in a frame that is addressed using the node's current (old) PHY ID and is encrypted using the encryption key appropriate to that node. The command includes, in the encrypted part of the frame, the new PHY ID for the node. This new PHY ID is linked to the existing encryption key, although the key could also be changed at the same time (in the same command as instructs the node to change address), to further increase security.

2. At the destination node the command is identified as being addressed to it, and is decrypted and interpreted. The destination node then adopts the new PHY ID and, if present, the new encryption key.

The present invention is preferably implemented over a shared data link, since in that situation it can provide additional advantages, but it could be implemented over links of other types. The data link could be any suitable form of data channel.

The applicant hereby discloses in isolation each individual feature described herein and any combination of two or more such features, to the extent that such features or combinations are capable of being carried out based on the present specification as a whole in the light of the common general knowledge of a person skilled in the art, irrespective of whether such features or combinations of features solve any problems disclosed herein, and without limitation to the scope of the claims. The applicant indicates that aspects of the present invention may consist of any such individual feature or combination of features. In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention.

CLAIMS

1. A communication system comprising:

a plurality of communication nodes connected by a data link;

a communication controller for allocating link-level addresses to the communication nodes whereby the nodes may be identified for communications over the link;

the communication controller being arranged to change from time to time the addresses allocated to each communication node and transmit the newly allocated address to the respective node in encrypted form.

2. A communication system as claimed in claim 1, wherein communications over the link comprise an address part indicating the address of the one of the nodes to which the respective communication is directed and a payload part.

3. A communication system as claimed in claim 2, wherein the address part is not encrypted.

4. A communication system as claimed in claim 2 or 3, wherein the payload part is encrypted.

5. A communication system as claimed in any preceding claim, wherein communications over the link are in the form of data packets.

6. A communication system as claimed in any preceding claim, wherein the communication system comprises a data distribution unit connected between the data link and at least one external data source for forwarding data from the data source to the nodes via the data link.

7. A communication system as claimed in claim 6, wherein the data distribution unit is arranged to forward the data to the nodes in a random or pseudo-random order.

8. A communication system as claimed in claim 6 or 7, wherein the data distribution unit is arranged to, at at least some times when it would otherwise not be transmitting data to the nodes, transmit over the link communications addressed to an address that is not allocated to any of the nodes.

9. A communication system as claimed in any preceding claim, wherein a node is arranged to store the address allocated to it and to ignore communications on the data channel addressed to addresses other than that address.

10. A communication system as claimed in any preceding claim, wherein the link is an Ethernet link.

11. A communication system as claimed in claim 10, wherein the link-level addresses are Ethernet PHY ID addresses.

12. A method for communicating data in a communication system, the communication system comprising a plurality of communication nodes connected by a data link and a communication controller; the method comprising:

the communication controller allocating link-level addresses to the communication nodes whereby the nodes may be identified for communications over the link;

the communication controller changing from time to time the addresses allocated to each communication node and transmitting the newly allocated address to the respective node in encrypted form.

13. A communication system substantially as herein described with reference to the accompanying drawings.

14. A method for communicating data substantially as herein described with reference to the accompanying drawings.

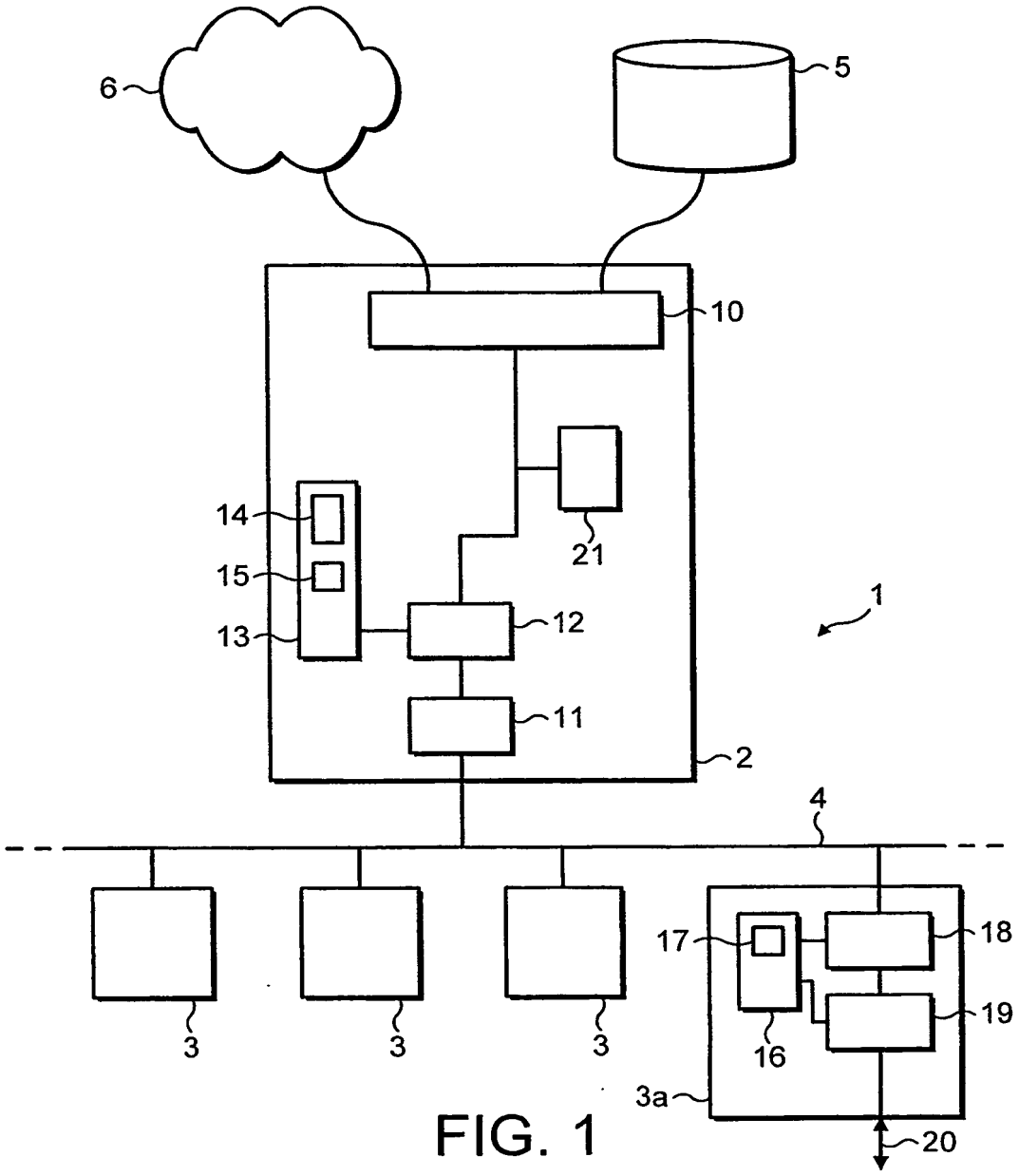


FIG. 1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/02825

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/00 H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 872 783 A (CHIN HON WAH) 16 February 1999 (1999-02-16) column 1, line 1 -column 3, line 44 abstract; figures 1-3,6A-6C ---	1-12
A	EP 0 472 836 A (IBM) 4 March 1992 (1992-03-04) column 1, line 1 -column 4, line 2 abstract; claims 1-12; figures 1-7 ---	1-12
A	US 6 028 933 A (HEER DANIEL N ET AL) 22 February 2000 (2000-02-22) column 1, line 1 -column 3, line 60 abstract; figures 1,2,6,7,23 --- -/--	1-12

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 December 2002	28. 01. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	ISMAR HADZIEFENDIC/JA

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/02825

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 344 978 A (NDS LTD) 21 June 2000 (2000-06-21) page 1, line 1 -page 10, line 15 abstract; claims 1-12; figures 1-3 ---	1-12
E	US 2002/133607 A1 (NIKANDER PEKKA) 19 September 2002 (2002-09-19) page 1, column 1 -page 3, column 2, line 47 abstract; claims 1-22; figures 1-3 -----	1-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 02/02825

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 13,14
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 13,14

The scope of protection for the subject matter defined by the claims 13 and 14 could not be unambiguously established.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/02825

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5872783 A	16-02-1999	NONE	
EP 0472836 A	04-03-1992	US 5276813 A	04-01-1994
		DE 69122013 D1	17-10-1996
		DE 69122013 T2	13-03-1997
		EP 0472836 A1	04-03-1992
		JP 1926222 C	25-04-1995
		JP 4241661 A	28-08-1992
		JP 6056596 B	27-07-1994
US 6028933 A	22-02-2000	NONE	
GB 2344978 A	21-06-2000	NONE	
US 2002133607 A1	19-09-2002	GB 2367986 A	17-04-2002
		WO 02076060 A2	26-09-2002

PATENT COOPERATION TREATY

PCT

RECEIVED
24 FEB 2004
WIPO PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION See Form PCT/IPEA/416	
300511WO/PRS		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB 2002/002825	03-05-2002	---
International Patent Classification (IPC) or national classification and IPC		
H04L 12/00, H04L 9/00		
Applicant		
Nokia Corporation et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☐ *(sent to the applicant and to the International Bureau)* a total of _____ sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s))
      _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☒ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☐ Box No. VI Certain documents cited
   - ☐ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand	Date of completion of this report
07-04-2003	11-02-2004
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. +46 8 667 72 88	Authorized officer Roger Bou Faisal /LR Telephone No. +46 8 782 25 00

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/IB 2002/002825

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of:

☐ international search (under Rules 12.3 and 23.1(b))
☐ publication of the international application (under Rule 12.4)
☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):*

☒ the international application as originally filed/furnished

☐ the description:
pages _____ as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☐ the claims:
pages _____ as originally filed/furnished
pages* _____ as amended (together with any statement) under Article 19
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☐ the drawings:
pages _____ as originally filed/furnished
pages* _____ received by this Authority on _____
pages* _____ received by this Authority on _____

☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/figs _____
☐ the sequence listing *(specify)*: _____
☐ any table(s) related to the sequence listing *(specify)*: _____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/figs _____
☐ the sequence listing *(specify)*: _____
☐ any table(s) related to the sequence listing *(specify)*: _____

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/IB 2002/002825

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application

☒ claims Nos. 13, 14

because:

☐ the said international application, or the said claims Nos. _____ relate to the following subject matter which does not require an international preliminary examination *(specify)*:

☐ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. _____ are so unclear that no meaningful opinion could be formed *(specify)*:

☐ the claims, or said claims Nos. _____ are so inadequately supported by the description that no meaningful opinion could be formed.

☒ no international search report has been established for said claims Nos. 13, 14

☐ the nucleotide and/or amino acid sequence listing does not comply with the standard provided for in Annex C of the Administrative Instructions in that:

the written form
- ☐ has not been furnished
- ☐ does not comply with the standard

the computer readable form
- ☐ has not been furnished
- ☐ does not comply with the standard

☐ the tables related to the nucleotide and/or amino acid sequence listing, if in computer readable form only, do not comply with the technical requirements provided for in the Annex C-*bis* of the Administrative Instructions.

☐ See Supplemental Box for further details.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/IB 2002/002825

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims	1-12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

Documents cited in the International Search Report:

D1: us 5872783, A
D2: EP 0472836, A
D3: US 6028933, A
D4: GB 2344978, A

The cited documents represent the general state of the art. The invention defined in claims 1- 12 is not disclosed by any of these documents.
The cited prior art does not give any indication that would lead a person skilled in the art to the claimed method and system for allocating and changing link-level addresses in a communications network. Therefore, the claimed invention is not obvious to a person skilled in the art.

Accordingly, the invention defined in claims 1- 12 is novel and is considered to involve an inventive step. The invention is industrially applicable.